ROB BONTA
Attorney General of California
LARA HADDAD, State Bar No. 319630
Supervising Deputy Attorney General
JENNIFER E. ROSENBERG, State Bar No. 275496
SHIWON CHOE, State Bar No. 320041
CHRISTOPHER J. KISSEL, State Bar No. 333937
Deputy Attorneys General
300 South Spring Street, Suite 1702
Los Angeles, CA 90013-1230
Telephone: (213) 269-6388
Fax: (916) 731-2124
E-mail: Christopher.Kissel@doj.ca.gov
*Attorneys for Defendant Rob Bonta, in his official capacity as Attorney General of California*

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| **NETCHOICE,**<br><br>Plaintiff,<br><br>**v.**<br><br>**ROB BONTA, in his official capacity as Attorney General of California,**<br><br>Defendant. | 5:24-cv-07885-EJD<br><br>**DECLARATION OF SERGE EGELMAN, PH.D., IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION**<br><br>Date: December 17, 2024<br>Time: 9 a.m.<br>Courtroom: 4, 5th Floor<br>Judge: Honorable Edward J. Davila<br>Trial Date: None Set<br>Action Filed: November 12, 2024 |

**DECLARATION OF SERGE EGELMAN, PH.D.**

I, Serge Egelman, Ph.D., declare and state as follows:

1. I submit this declaration in support of Defendant's Opposition to Plaintiff's Motion for Preliminary Injunction.

**BACKGROUND & QUALIFICATIONS**

2. I am the Research Director of the Usable Security & Privacy Group at the International Computer Science Institute (ICSI), which is a non-profit research institute affiliated with the University of California, Berkeley. I also hold a position as a research scientist within the Electrical Engineering and Computer Sciences (EECS) Department at the University of California, Berkeley. I received my Ph.D. from Carnegie Mellon University's School of Computer Science. My research has been cited over 13,000 times, and my h-index—the most common metric for scientific impact[1]—is over 50.[2]

3. I have been performing research into online privacy for over twenty years. My research focuses on the interplay of online privacy, computer security, and human factors. In short, I study: consumer privacy and security decision making; consumer privacy preferences; privacy and security expectations; and how those expectations comport with reality (e.g., by performing technical analyses of online services and other software to examine privacy and security practices). This research involves both technical knowledge to build tools for use in measurement studies (e.g., observational studies of how user data is collected and shared in practice), as well as a deep understanding of how to apply social science methodologies (e.g., human subjects research, surveys, interviews, randomized controlled trials, etc.). I have served as an invited expert for several web standards efforts that pertained to privacy and security, and have received over a dozen awards from the research community (including: privacy research awards from two European data protection authorities, AEPD in Spain and CNIL in France; the USENIX

[1] J.E. Hirsch, An index to quantify an individual's scientific research output, Proc. Natl. Acad. Sci. U.S.A. 102 (46) 16569-16572, https://doi.org/10.1073/pnas.0507655102 (2005).

[2] https://scholar.google.com/citations?user=WN9t4n0AAAAJ&hl=en.

Security Symposium Distinguished Paper Award, from one of the top academic computer security conferences; the Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies; and seven paper awards from the ACM Special Interest Group on Computer-Human Interaction [SIGCHI], the top human-computer interaction conference). I have also been repeatedly invited to speak at the FTC's annual "PrivacyCon" event based on my laboratory's research.

4. Over the past decade, my laboratory has been studying the mobile application ("app") ecosystem, which has included building tools to detect when personal information is accessed by mobile apps and the third parties with whom they share it. We have used these tools in peer-reviewed published research studies about consumer privacy, including examining mobile apps' compliance with various privacy regulations and platform policies.

5. One research study performed by my laboratory demonstrated that a majority of child-directed Android apps appeared to be violating the federal Children's Online Privacy Protection Act of 1998 ("COPPA") in various ways,[3] which led to major policy shifts by both Google and Apple, makers of the two leading mobile platforms. I have since been invited to give keynotes at several international conferences on child development and technology as an expert on online privacy as it pertains to children. I have also testified before the U.S. Senate on how COPPA can be improved to match the realities of modern technology, and have been asked to provide feedback on draft legislation from members of both houses of Congress.

6. My *curriculum vitae*, which sets forth my experience and credentials more fully, is attached as Exhibit A.

7. I have testified as an expert in the following cases:

- *Garner v. Amazon.com, Inc.*, No. 2:21-cv-00750 (W.D. Wa.)
- *Lopez et al. v. Apple, Inc.*, No. 4:19-cv-04577-JSW (N.D. Cal.)

[3] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale.* Proceedings on Privacy Enhancing Technologies (PoPETS), 2018(3):63–83.

- *Martinez et al. v. D2C, LLC d/b/a UNIVISION NOW*, No. 1:23-cv-21394-RNS (S.D. Fla.).
- *Bloom v. Zuffa LLC*, No. 2:22-cv-00412-RFB-BNW (D. Nev.)
- *Clark, et. al. v. Yodlee, Inc.*, No: 3:20-cv-05991-SK (N.D. Cal.).
- *Czarnionka v. The Epoch Times Association, Inc.*, No. 1:22-cv-6348 (S.D.N.Y.)
- *Frasco v. Flo Health, et al.*, No. 3:21-cv-00757 (N.D. Cal.).
- *Hart v. TWC Prod. & Tech. LLC*, No. 20-cv-03842-JST (N.D. Cal.)
- *In re Vizio, Inc., Consumer Privacy Litig*., No. 8:16-ml-02693-JLS-KES (C.D. Cal.)
- *In re Linkedin User Privacy Litigation*, No. 5:12-cv-03088 EJD (N.D. Cal.)
- *In re Netflix Privacy Litigation*, Case No.: 5:11-cv-00379 EJD (N.D. Cal.)
- *District of Columbia v. Town Sports International*, *LLC*, No. 2020 CA 003691 B (D.C. Sup. Ct. 2020)

8. I am being compensated in the above-entitled case at an hourly rate of $400/hour for preparing this declaration. My compensation is not in any way dependent on the outcome of this or any related proceeding.

9. The opinions in this declaration are my expert opinions, which are based on my education and training, my peer-reviewed published research and the research of others, my knowledge of relevant technologies (including my reading of public technical documents offered by NetChoice's members about their capabilities), as well as my reading of the legislation.

10. Portions of this declaration are taken from a declaration I authored for the California Attorney General's Office in another matter, *NetChoice v. Bonta* (N.D. Cal., Case No. 5:22-cv-08861-BLF). I include those portions here in case they aid the Court in understanding how social media sites and applications are designed to increase engagement by minors and adults.

11. If called to testify, I could and would testify competently to the truth of the matters discussed in this declaration.

**OPINIONS**

12. I have reviewed SB 976, California's Protecting Our Kids from Social Media Addiction Act ("the Act").

13. I understand that SB 976 includes several features aimed at curbing excessive use of social media among children and adolescents, including by, among other things, (1) prohibiting Internet-based services or applications that provide user-generated content from providing addictive content feeds to minors absent verifiable consent; (2) prohibiting such services or

applications from sending "push notifications"[4] to minor users during the school day and between the hours of 12 a.m. to 6 a.m. absent verifiable parental consent; and (3) requiring that such service or applications adhere to certain default settings (including requiring that the default feed provided to a child not be selected or prioritized for display based on information provided by the user or associated with the user's device, other than the user's age or status as a minor).

14. In my expert opinion, there is widespread use by social media companies and other online service providers of algorithmic content curation designed to encourage children to spend more time or money engaging with online services or otherwise acting against their best interests. The Act's provisions aimed at limiting minors' excessive use of social media are reasonable and technically feasible to adopt.

## I. DRIVING ONLINE USER ENGAGEMENT

15. In this section I provide background on how online services are monetized through the collection of users' personal information, how this incentivizes "engagement," and how algorithms are used to engage users and/or manipulate them into acting against their interests.

### A. Collection and Use of Personal Information Online

16. The "free" Internet is subsidized through the collection of users' personal information for both advertising and analytics purposes. In the case of advertising, this means showing Internet users ads that are specifically tailored to their inferred interests. In the case of analytics, this means observing how users interact with the service in order to maximize its profitability (e.g., strategically placing in-app purchase opportunities based on users' in-app behaviors, identifying the users most likely to buy expensive items based on their inferred demographics, manipulating users into spending more time using a service, etc.). In other cases,

---

[4] "Push notifications" refer to notification messages that appear on consumers' devices as a result of apps attempting to get the user's attention. They generally appear in the device's "notification center," "status bar," or other dedicated area of the screen, and are used to encourage the user to take a specific action when using the notifying app (e.g., reading a new message, viewing a special offer, etc.).

this may mean selling the user data to third parties so that they may perform these activities and other yet-unknown use cases.

17. Because so much of the Internet is supported by advertisements, one key metric that online services use is known as "engagement," which refers to the amount of time that consumers spend using a service or the frequency of interactions that consumers have with that service. That is, the more time consumers spend using a service that displays ads, the more ads that consumers are likely to be shown, and therefore the more revenue that the service can derive by charging advertisers to show those ads. Similarly, the more personal information that consumers share with a service, the more likely those consumers are to see "relevant" ads, and therefore the more likely they are to click those ads.

18. Thus, many services collect analytics data to measure engagement and then use this data to optimize and develop features that are likely to lead to greater levels of engagement (i.e., more time spent using the service or more monetizable personal information divulged to the service).[5] More engagement results in more advertisements being viewed (due to more time spent using the service), resulting in more revenue.

19. Advertisements are targeted at users based on inferences about those users' interests. Individual users' interests are inferred based on data automatically collected from them: the services they use, how they use them, from where they use them, and so forth. In short, online and offline activities are tracked, which allows companies to maintain detailed profiles of individual user behavior, which in turn is used to predict users' interests, preferences, and even demographics. The collected information may be used to predict a consumer's religion, health conditions, sexual orientation, or political affiliation; some of this information may be revealed by the device's location alone (e.g., where they live, who they live with, where they work, etc.), or

---

[5] Filippo Menczer, "How 'Engagement' Makes You Vulnerable to Manipulation and Misinformation on Social Media." *The Conversation,* September 20, 2021, https://theconversation.com/how-engagement-makes-you-vulnerable-to-manipulation-and-misinformation-on-social-media-145375. Accessed: October 22, 2024.

even by just the name of the app that is being used (e.g., revealing sexual orientation, religion, age, or socioeconomic status).

20. For example, Meta, a NetChoice member, uses the personally identifiable information that it collects to build dossiers about users' interests, preferences, activities (both online and offline), location trails, and even social relations. These dossiers are then used to determine which advertisements to show to which users, when an advertiser pays Meta to show its advertisements to their users.[6] For example, when I accessed the "Ads Manager" interface to go through the steps of posting a targeted advertisement on Facebook (as any advertiser would), I was given the option to target an advertisement based on demographics, interests, and prior observed behaviors (Figures 1–3).

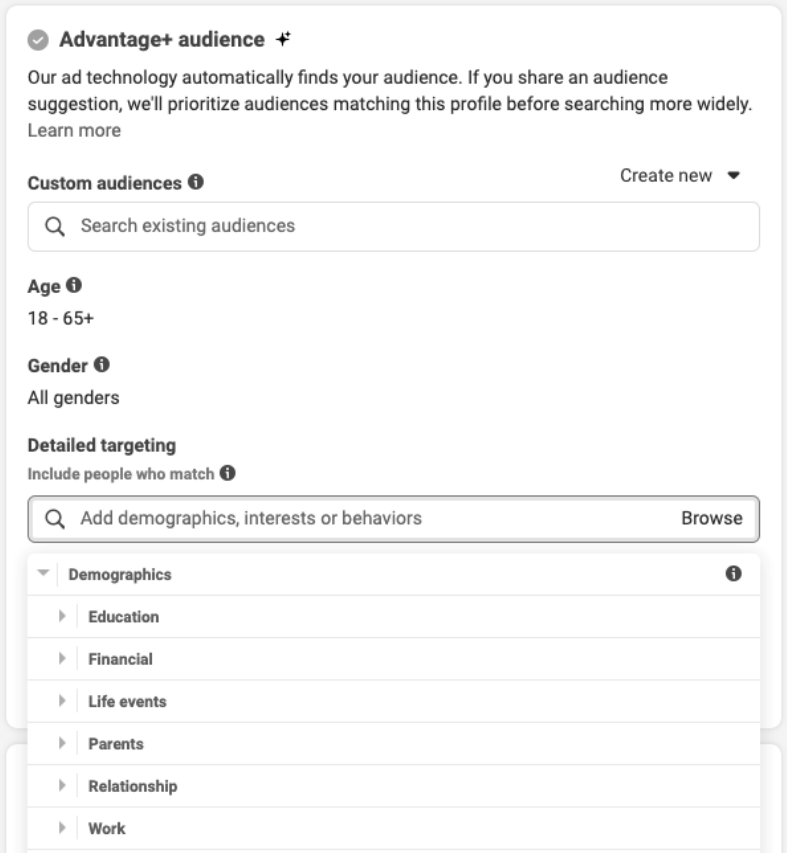


Figure 1: Facebook Ads Manager showing demographic targeting criteria. Source: https://adsmanager.facebook.com/.

[6] Meta. "Audience Ad Targeting." *Meta Ads,* https://www.facebook.com/business/ads/ad-targeting. Accessed: October 22, 2024.

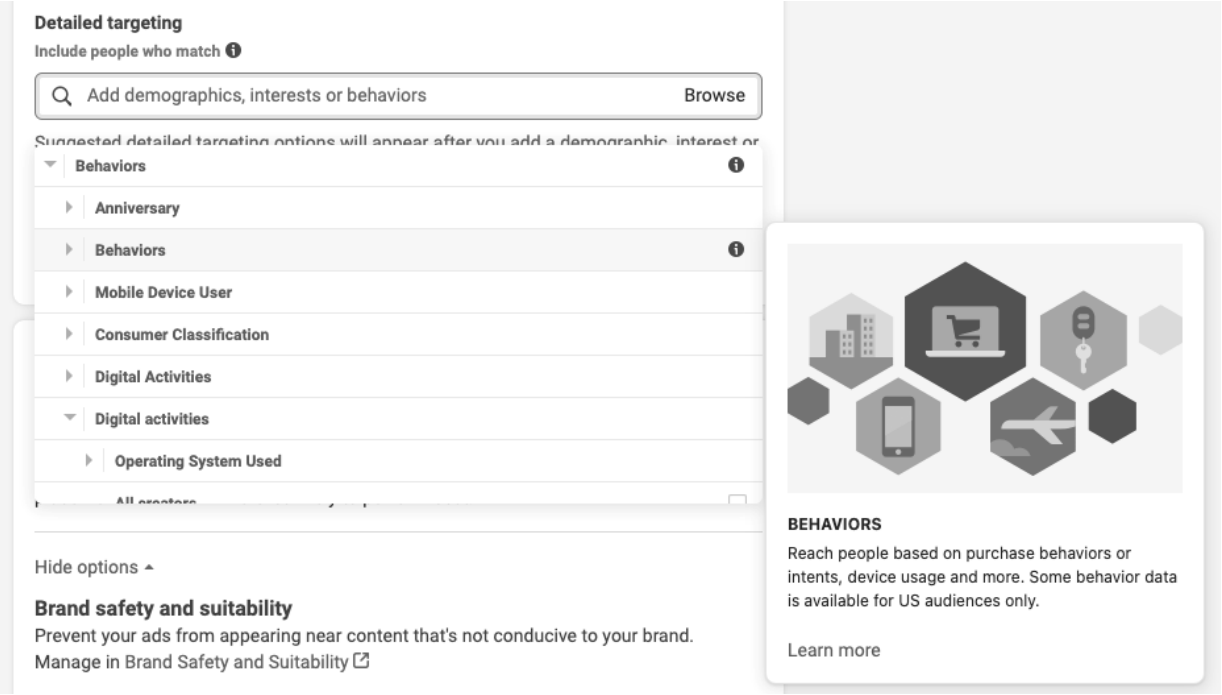


Figure 2: Facebook Ads Manager showing behavioral targeting criteria.
Source: https://adsmanager.facebook.com/.

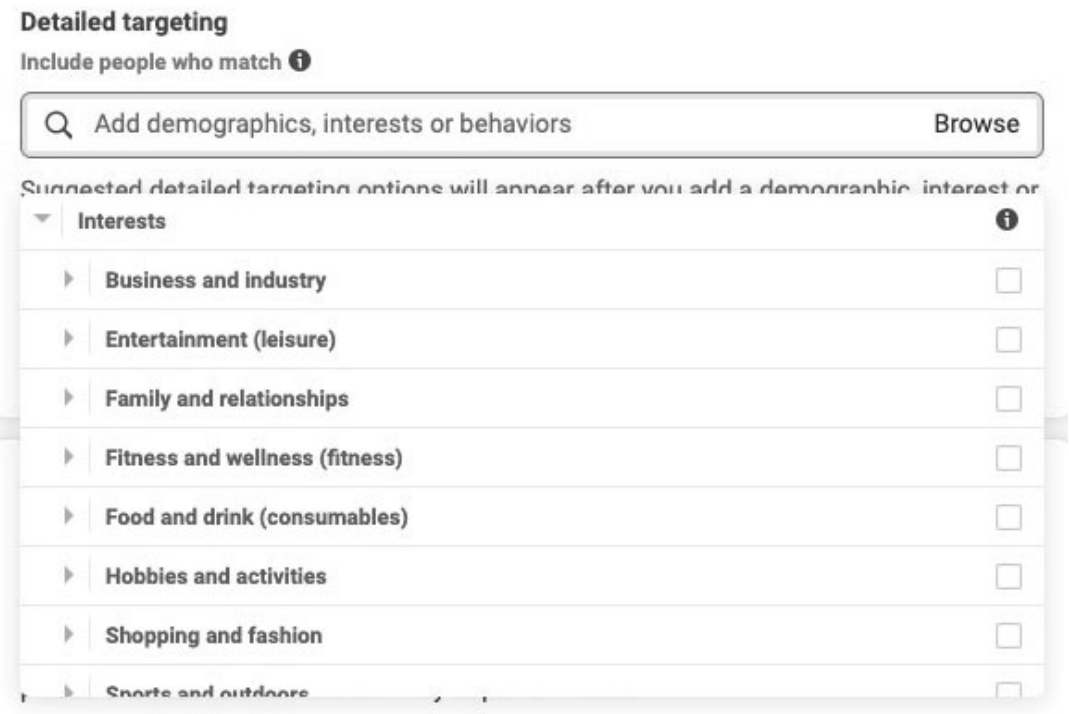


Figure 3: Facebook Ads Manager showing interest-based targeting criteria.
Source: https://adsmanager.facebook.com/.

21. Specifically, expanding these options shows very fine-grained ad targeting criteria that Meta's advertisers can use to target ads at specific Facebook users.[7] While some of these data points are based on information that Facebook users have posted to Facebook, many others are based on information gleaned from third parties or from metadata gleaned from users' usage behaviors. These fine-grained ad-targeting criteria include sensitive personal information such as:

a. Demographics
   i. Age
   ii. Gender
   iii. Geographic location
   iv. Education level
   v. Field of study (e.g., major)
   vi. School
   vii. When someone went to college
   viii. Income
   ix. Life events (e.g., anniversary, travel, birthday, new job, new relationship, recent engagement, newlyweds, recently moved, etc.)
   x. Parental status (including ages of children)
   xi. Relationship status
   xii. Employer
   xiii. Field of employment
   xiv. Job title

b. Interests
   i. Specific businesses and industries
   ii. Entertainment interests (e.g., games played, movies and television watched, music interests, reading preferences, etc.)

[7] Meta. "Facebook Ads Manager." https://adsmanager.facebook.com/. Accessed: October 22, 2024.

iii. Family interests (e.g., parenting, marriage, etc.)

iv. Fitness interests (e.g., bodybuilding, exercise preferences, yoga, etc.)

v. Food and drink preferences (including restaurant preferences)

vi. Hobbies (e.g., arts and music, current events, politics, home and garden, pets, travel, vehicles, etc.)

vii. Shopping and fashion

viii. Sports and outdoors

ix. Technology

c. Behaviors

i. Recent purchases

ii. Device usage/ownership

iii. Specific software used

iv. Online activities

v. Travel history

vi. Transit behaviors (e.g., commuters, users of public transit, etc.)

22. Online services are able to offer advertisers such fine-grained ad targeting options due to the breadth of the data they collect from individual Internet users. For example, when people create Facebook profiles and use Facebook, they share a wealth of personal information with Meta: their names, addresses, contact information, gender, preferences (e.g., via use of the "like" button and membership in affinity groups), relationship information, birthdates, and many other types of information. To quote Mark Zuckerberg on peoples' willingness to provide Facebook sensitive information unquestioningly, "[p]eople just submitted it. I don't know why. They 'trust me.'"[8]

**23.** Tracking of users' online behaviors is made possible by "persistent identifiers."

[8] Laura Raphael. "Mark Zuckerberg Called People Who Handed Over Their Data 'Dumb F****'." *Esquire*, March 19, 2018, https://www.esquire.com/uk/latest-news/a19490586/mark-zuckerberg-called-people-who-handed-over-their-data-dumb-f/. Accessed: October 22, 2024.

An identifier is any piece of information that allows an individual—or device—to be uniquely identified. "Persistent" identifiers are identifiers that tend to not change over time.[9] For example, motor vehicles have persistent identifiers in the form of license plates: a license plate uniquely identifies a vehicle, and vehicles tend to have the same license plates over time. If someone records all the license plates at a particular place over time, they can determine how many times in that period any individual vehicle was there (and thus infer their operators' activities). Similarly, if license plates are recorded at many different locations and that data is combined, one could reconstruct the movements of individual vehicles. Thus, combining a persistent identifier with information about where that identifier was observed (e.g., a website or mobile app) allows a data recipient to reconstruct an individual's activities. Using this knowledge, one could infer information about a person's routines, preferences, demographics, and even relations and social connections by tracking their persistent identifier. It is for this reason that persistent identifiers, including ones that identify personal devices—because such devices tend to be used by one individual—are categorized as personal information under various privacy laws (e.g., the California Consumer Privacy Act ("CCPA"),[10] COPPA,[11] the federal Health Insurance Portability and Accountability Act ("HIPAA"),[12] the European Union's General Data Protection Regulation ("GDPR"),[13] the Gramm-Leach-Bliley Act ("GLBA")[14]).[15]

24. While consumers are overwhelmingly opposed to this type of tracking and the profiling and resale of their information that it supports (one study of U.S. consumers found that

---

[9] https://www.nnlm.gov/guides/data-glossary/persistent-unique-identifier.

[10] Cal. Civ. Code § 1798.140(15).

[11] 15 U.S.C § 6501(8)(F).

[12] 45 C.F.R. § 164.514(b)(2)(i).

[13] GDPR Art. 4 (1).

[14] 16 C.F.R. § 313.3.

[15] See, e.g., https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information.

up to 86% do not want ads that are tailored based on their online activities),[16] consumers nonetheless continue to engage with services that appear to conflict with their stated privacy preferences. This is known as the "privacy paradox." Some stakeholders like to point out this disconnect and use it to disingenuously claim that it means that consumers do not "really" care about privacy. But the published research on the privacy paradox demonstrates that this argument is incorrect, and that there are several rational explanations for the privacy paradox, which include lack of awareness of data collection methods, poor usability, mismatched incentives, and perceived lack of agency.

25. In many cases, consumers simply do not understand when they are making decisions that will impact their privacy. For example, in a series of studies that I co-authored,[17] we presented subjects with different search engine interfaces, including one that annotated search results with privacy information; subjects were instructed to use the search engine to buy items from merchants of their choice. While all subjects expressed strong privacy preferences in a survey administered prior to the study (i.e., subjects were specifically screened for strong privacy preferences, so that we could explicitly test whether interface design impacted their ability to act on those preferences), we observed that without information about privacy practices presented in

---

[16] J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy (2009). "Americans Reject Tailored Advertising and Three Activities That Enable It." https://doi.org/10.2139/ssrn.1478214.

[17] Janice Y. Tsai Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. "The effect of online privacy information on purchasing behavior: An experimental study." *Information systems research* 22, no. 2 (2011): 254-268; Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. "Timing is everything? The effects of timing and placement of online privacy indicators." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 319-328. 2009; Julia Gideon, Lorrie Cranor, Serge Egelman, and Alessandro Acquisti. "Power strips, prophylactics, and privacy, oh my!" In *Proceedings of the Second Symposium on Usable privacy and security*, pp. 133-144. 2006.

an easily-accessible manner, subjects made purchases from the cheapest merchants (with the worst privacy practices). Whereas when search results were annotated with privacy ratings, subjects were significantly more likely to make purchases from merchants with more agreeable privacy policies (i.e., better aligned with participants' stated privacy preferences), even paying more money to do so. These and other studies demonstrate that people often act in ways that seem contrary to their stated privacy preferences when they are not fully aware of a business's privacy practices (e.g., due to the well-documented problems with the "notice and consent" framework, i.e., expecting consumers to read and understand privacy policies, which I describe in subsequent sections).

26. In other cases, convoluted user interfaces make it difficult for consumers to understand how to make privacy-protective decisions. This poor usability often results in consumers sharing personal information without ever being aware of it. For example, while studies have shown that consumers have concerns about sharing personal information with the wrong audiences on social media, they nonetheless continue to overshare,[18] which has been shown to be the result of difficult-to-use privacy settings interfaces (or mismatches between the design of those interfaces and users' mental models).[19] One early study on the use of Facebook found that while participants expressed strong privacy preferences, they nonetheless shared sensitive information because more than one-in-five did not understand what Facebook's privacy settings did or how to use them, and therefore did not change them from the overly-permissive

---

[18] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and privacy: it's complicated. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12). Association for Computing Machinery, New York, NY, USA, Article 9, 1–15. https://doi.org/10.1145/2335356.2335369.

[19] Jennifer King, Airi Lampinen, and Alex Smolen. 2011. Privacy: is there an app for that? In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). Association for Computing Machinery, New York, NY, USA, Article 12, 1–20. https://doi.org/10.1145/2078827.2078843.

defaults.[20] In a study of file-sharing software, researchers discovered that due to convoluted privacy settings interfaces, many users were inadvertently sharing their entire hard drives.[21] In a study of tools provided by the advertising industry to opt out of behavioral advertising on websites, the researchers observed:

> "Participants found many tools difficult to configure, and tools' default settings were often minimally protective. Ineffective communication, confusing interfaces, and a lack of feedback led many participants to conclude that a tool was blocking [online behavioral advertising] when they had not properly configured it to do so. Without being familiar with many advertising companies and tracking technologies, it was difficult for participants to use the tools effectively."[22]

27. Incentives are also important when studying privacy tradeoffs. Privacy decisions are not made in a vacuum: that consumers engage with services that violate their privacy preferences is often an indictment of the lack of market choice rather than an indication that consumers are behaving hypocritically. Similarly, privacy is often not the only consideration: if the costs of protecting one's privacy are unreasonably high (e.g., time invested learning to correctly use privacy settings, monetary costs, abstaining from social life, etc.), many consumers will engage with privacy-violative services because they cannot afford the alternatives. For example, I value my free time, but that I still show up to work does not make me a hypocrite.

---

[20] Alessandro Acquisti and Ralph Gross. "Imagined communities: Awareness, information sharing, and privacy on the Facebook." In *Privacy Enhancing Technologies: 6th International Workshop*, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers 6, pp. 36-58. Springer Berlin Heidelberg, 2006.

[21] Nathaniel S. Good and Aaron Krekelberg. 2003. "Usability and privacy: a study of Kazaa P2P file-sharing." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. Association for Computing Machinery, New York, NY, USA, 137–144. https://doi.org/10.1145/642611.642636.

[22] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. "Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising." In *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 589-598. 2012.

28. Similarly, when faced with the choice between protecting their privacy or engaging with their peers online, many younger people will choose the latter, despite the known privacy risks. Many studies have shown that despite the known privacy risks, many young people continue to use social media due to the fear of missing out.[23]

29. Finally, many consumers simply do not believe they have agency when it comes to making online privacy decisions: because many believe that their privacy preferences will not be honored no matter the actions that they take, many choose to engage with privacy-violative services to extract benefits, believing that they will end up paying the privacy costs regardless. A 2015 consumer survey concluded the following:

> "[A] majority of Americans are resigned to giving up their data—and that is why many appear to be engaging in tradeoffs. Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them. Our study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened."[24]

---

[23] Vittoria Franchina, Mariek Vanden Abeele, Antonius J. Van Rooij, Gianluca Lo Coco, and Lieven De Marez. "Fear of missing out as a predictor of problematic social media use and phubbing behavior among Flemish adolescents." *International journal of environmental research and public health* 15, no. 10 (2018): 2319; Dmitri Rozgonjuk, Cornelia Sindermann, Jon D. Elhai, and Christian Montag. "Fear of Missing Out (FoMO) and social media's impact on daily-life and productivity at work: Do WhatsApp, Facebook, Instagram, and Snapchat Use Disorders mediate that association?." *Addictive Behaviors* 110 (2020): 106487; Ine Beyens, Eline Frison, and Steven Eggermont. "'I don't want to miss a thing': Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress." *Computers in Human Behavior* 64 (2016): 1-8.

[24] Joseph Turow, Michael Hennessy, and Nora Draper. "The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation." *Available at SSRN 2820060* (2015).

30. A study specifically on young people and the privacy paradox observed:

> "Based on focus group interviews, we considered how young adults' attitudes about privacy can be reconciled with their online behavior. The "privacy paradox" suggests that young people claim to care about privacy while simultaneously providing a great deal of personal information through social media. Our interviews revealed that young adults do understand and care about the potential risks associated with disclosing information online and engage in at least some privacy-protective behaviors on social media. However, they feel that once information is shared, it is ultimately out of their control. They attribute this to the opaque practices of institutions, the technological affordances of social media, and the concept of networked privacy, which acknowledges that individuals exist in social contexts where others can and do violate their privacy."[25]

31. Similarly, users continue to use apps that they find "creepy" due to a sense of learned helplessness: they do not believe that they have the power to control who receives their personal information when they participate in the digital economy.[26] Sometimes, online services are specifically designed to manipulate users into continuing to use them through the use of specially designed algorithms.

**B. Algorithms**

32. An algorithm is simply a sequence of operations: there is often an input, calculations are performed on that input, and then the results of those calculations are provided as output. Within the context of online services, algorithms are used for everything from recommending content to users to inferring a user's preferences and traits for purposes such as targeted advertising. There is no such thing as a "neutral" algorithm: algorithms are designed for specific purposes. One algorithm might be designed to show ads that maximize ad revenue, whereas another might be designed to optimize engagement through content recommendations;

---

[25] Eszter Hargittai, and Alice Marwick. "'What can I really do?' Explaining the privacy paradox with online apathy." *International journal of communication* 10 (2016): 21.

[26] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421.

other algorithms might be used for more mundane tasks, such as sorting items chronologically or alphabetically. That is, the logic used to display content to users will always rely on an algorithm, even if that algorithm is as simple as displaying items chronologically. Though in practice, the algorithms used by social media companies are generally much more complex, because they are designed to drive engagement. For example, in determining the tweets that appear in a user's feed (of the hundreds of millions sent per day), X, the social media service formerly known as Twitter, weighs factors such as the number of likes, retweets, social relations, recency, perceived topic relevance, and use of embedded media, among other factors.[27]

33. While some algorithms might make objective decisions (e.g., correctly sorting a list of items by date), others are subjective and therefore less straightforward to audit for correctness (e.g., recommending content and choosing advertisements to display).[28] Algorithms are increasingly being used to make decisions about individuals that can have profound consequences, such as extending credit, housing, insurance, employment, or school admissions; in many cases there is little transparency or recourse surrounding these decisions, as they are made automatically and opaquely, and may also use incorrect or biased data.[29] Most adults do not understand if, when, and how these decisions are being made, children less so.

34. One class of algorithms, known as "recommender systems," are specifically

---

[27] Josiah Hughes, "How the Twitter Algorithm Works [2023 Guide]." Hootsuite, December 14, 2022. https://blog.hootsuite.com/twitter-algorithm/.

[28] Zeynep Tufekci, "Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency," Colorado Technology Law Journal 13, no. 2 (2015): 203-218.

[29] Danielle Keats Citron and Pasquale, Frank A., "The Scored Society: Due Process for Automated Predictions" (2014). Washington Law Review, Vol. 89, 2014, p. 1-, U of Maryland Legal Studies Research Paper No. 2014-8, Available at SSRN: https://ssrn.com/abstract=2376209.

designed to choose what content to show to which users.[30] In many cases, these algorithms are designed to optimize for user engagement: factoring in the content that a user previously engaged with to determine what new content to show the user to get them to continue engaging with the service. Obviously, the personal information collected from consumers (described earlier) is of great utility in determining what content consumers are likely to find engaging.

35. Algorithms that are optimized for increasing user engagement can also result in harm to consumers. For example, there was public outrage when the public learned that Facebook was using its content recommendation algorithms to intentionally cause emotional distress among its users. (Facebook researchers found that emotionally charged posts were more likely to lead to user engagement; Facebook thus has an incentive to use its algorithms to prioritize showing users posts that are likely to evoke emotional responses.)[31] Recent research has shown that misinformation leads to greater levels of engagement for social media platforms: "(i) misinformation sources evoke more outrage than do trustworthy sources; (ii) outrage facilitates the sharing of misinformation at least as strongly as sharing of trustworthy news; and (iii) users are more willing to share outrage-evoking misinformation without reading it first."[32]

36. In my own research, I have observed that very few Internet users understand that their social media feeds are being curated based on complex algorithms designed to optimize for engagement. Indeed, many consumers erroneously assume that these feeds are chronological. Children may be even less likely to understand that their content feeds are being algorithmically

---

[30] Konstan JA, Riedl J (2012). "Recommender systems: from algorithms to user experience" (PDF). User Modeling and User-Adapted Interaction. 22 (1–2): 1–23. doi:10.1007/s11257-011-9112-x. S2CID 8996665.

[31] Kashmir Hill, "Facebook Manipulated 689,003 Users' Emotions For Science." Forbes, June 28, 2014. https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/.

[32] Killian L. McLoughlin et al., "Misinformation exploits outrage to spread online." *Science* 386,991-996(2024). doi:10.1126/science.adl2829.

curated, and that the manner in which they are being curated are designed to manipulate them.

### C. Other Drivers of Engagement

37. In addition to curating content or choosing which ads to display, there are other drivers of engagement that online services regularly use. For example, app notifications may be used to remind the user that they have not used a specific app in a long time or to communicate a personalized promotion. Gamification, through the use of quantifiable rewards, is another way that social media services drive engagement (e.g., enticing users to chase after more "likes" or "followers"). Or, as another example, a video streaming website may automatically play the next recommended video in order to entice the viewer to continue using the service.

## II. Special Concerns Regarding Children's Privacy

38. Data monetization is even more concerning when the data comes from children, who are unlikely to understand that this is happening, much less consent to it, but who could potentially face enormous impacts due to future usage of this data. This data may be used for manipulative marketing campaigns, but also may feed biased and unaccountable algorithms that use it to make decisions about a child's future, not to mention outright malicious uses of the data (e.g., non-custodial parents purchasing location data to geolocate a child).

39. In 2016 my research team decided to look at how well mobile apps directed at children appeared to be complying with COPPA, which has been in effect since 2000. We wrote bespoke instrumentation for the Android platform that allows us to run mobile apps and monitor exactly what personal information those apps access and with whom they share it.[33] We also used

---

[33] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov. "Android permissions remystified: A field study on contextual integrity." In *Proceedings of the 24th USENIX Security Symposium (USENIX Security 15)*, pages 499–514, Washington, D.C., Aug. 2015. USENIX Association; P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov. "The feasibility of dynamically granted permissions: aligning mobile privacy with user preferences." In *Proceedings of the 2017 IEEE Symposium on Security and*

(continued…)

our instrumentation to determine whether transmissions containing personal information were performed securely and confidentially.

40. Starting in late 2016, we began downloading as many free apps in the "Designed for Families" (DFF) program as we could find, which ended up being just under 6,000 apps.[34] The DFF program is a section of the Play Store, Google's centralized Android app market, which is exclusively for apps that are directed to children. Mobile app developers must participate in the program when they upload their app and disclose to Google that it is directed at children. As part of the program, they must affirm to Google that their app is in compliance with COPPA. Our goal was to evaluate whether that appeared to be the case in practice.

41. Of the child-directed apps that we tested, more than half appeared to be violating COPPA in one way or another: 5% collected location or other contact information and 19% collected personal information without verifiable parental consent and shared it with third parties whose public disclosures indicated they would use them for prohibited purposes (e.g., behavioral advertising); 40% transmitted personal information insecurely. Separately, 39% appeared to be

---

*Privacy*, Oakland '17. IEEE Computer Society, 2017; P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, K. Beznosov, and S. Egelman. "Contextualizing privacy decisions for better prediction (and protection)." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems,* CHI '18, pages 1–13, New York, NY, USA, 2018. Association for Computing Machinery; J. Reardon, A. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman. "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System." In *Proceedings of the 24th USENIX Security Symposium, USENIX Security '19,* Berkeley, CA, USA, 2019. USENIX Association. We wrote our tools for Google's Android platform only because it is open source: having the source code for the operating system allowed us to modify it for this purpose; at the time, we didn't look at Apple's iOS simply because we didn't have the source code to add the same level of instrumentation.

[34] Reyes *et al.*, *supra* note 3.

violating Google's platform policies (i.e., an example of industry self-regulation) surrounding the collection of persistent identifiers for advertising and analytics purposes.[35]

42. We also examined mobile apps that had been certified by the COPPA Safe Harbor programs, meaning that the app developer claimed to participate in a private FTC-approved compliance-certification program.[36] (We found it extraordinarily difficult to identify which mobile apps had actually been certified; none of the programs we contacted were willing to share lists of apps with us, and most of their websites did not provide this information.) Of the 237 apps we found that claimed to be Safe Harbor certified, 64% appeared to violate Google's policies on transmitting identifiers for advertising/analytics purposes, 33% transmitted personal information to prohibited third parties, and 32% transmitted personal information insecurely. We concluded that the apps that we examined, which claimed to be certified as COPPA-compliant by Safe Harbor programs, were no more likely to protect children's personal information than apps that had not been certified by these programs.[37] (This result is consistent with prior research on adverse selection in industry self-regulatory certification programs.)[38]

43. Thus, based on this research, I have come to the conclusion that voluntary industry self-regulatory children's privacy programs are ineffective, and do not lead to better outcomes for consumers.[39]

44. Similarly, through this research, I identified several additional gaps in regulation (beyond the inadequacy of the Safe Harbor programs), that I recommended be fixed in my U.S.

---

[35] *Ibid.*

[36] 16 C.F.R. § 312.11.

[37] Reyes *et al.*, *supra* note 3.

[38] Benjamin Edelman. "Adverse selection in online 'trust' certifications." In *Proceedings of the 11th International Conference on Electronic Commerce*, pp. 205-212. 2009.

[39] Egelman, S., 2023. "Informing Future Privacy Enforcement by Examining 20+ Years of COPPA." Harvard Journal of Law & Technology, 37(3).

Senate testimony.[40] Particularly relevant here are COPPA's "internal operations" exemption[41] and "actual knowledge" standard.[42]

45. Generally, websites and other online services must obtain verifiable parental consent before disclosing children's personal information to third parties, unless it is to support the service's internal operations and is not used for any other purpose. However, from a technical standpoint, most internal operations do not strictly require the collection of persistent identifiers that can be used to track children's activities across different services. In fact, both major platforms provide guidelines on how software developers can perform these activities *without* collecting advertising identifiers or non-resettable device identifiers.[43] For example, by definition, "contextual advertising" involves showing consumers ads *without* using data previously collected about them, and therefore no personal information is needed to show contextual ads. To prevent one user from being shown the same ad repeatedly (known as "frequency capping"), a session-based or installation-based identifier should be used, such that the collected data cannot be used to track the user across other services.

46. Nonetheless, in the course of my research, I have noticed that many privacy policies associated with child-directed services use the phrase "internal operations," when describing the flow of children's personal information to third parties. In many of these cases,

---

[40] U.S. Congress. Hearing of the Subcommittee on Consumer Protection, Product Safety, and Data Security of the Committee on Commerce, Scient, and Transportation. Hearing on "Protecting Kids Online: Internet Privacy and Manipulative Marketing." Testimony of Serge Egelman, 2021. https://www.commerce.senate.gov/services/files/0DC78E9D-88B2-4D54-8F4A-AE7B4C7D0EF6.

[41] 15 U.S.C. § 6501(4)(A).

[42] 15 U.S.C. § 6501(4)(B).

[43] Google, "Best Practices for Unique Identifiers." April 6, 2023. https://developer.android.com/training/articles/user-data-ids; Apple, "User Privacy and Data Use." 2023. https://developer.apple.com/app-store/user-privacy-and-data-use/.

these third parties are advertisers whose public disclosures indicate that they may use the data for COPPA-prohibited purposes. Thus, I have concluded that for many developers, the phrase "internal operations" appears to be a shibboleth used to justify privacy-invasive practices.

47. Secondly, COPPA's "actual knowledge" standard, by which it must be shown that an individual within these third-party organizations knew that they received data from children under age 13, incentivizes data recipients to simply look the other way if and when they receive children's personal information, even when those third-party transmissions also include the names of the apps or websites that are transmitting them the data. Many of these data recipients are advertising and/or analytics companies that publicly advertise their abilities to target ads based on inferring the demographics of users of the services sending them data. Furthermore, there are many commercial services that purport to provide the target demographics of a given mobile app or a website, and thus determining whether or not a service is directed at children is readily ascertainable.

48. For example, ironSource is a targeted advertising company that we observed receiving personal information from child-directed apps.[44] Their privacy policy stated they did not knowingly receive personal information from children under 13, a point which was reiterated to my laboratory in a letter from their general counsel.[45] In my response, I pointed out that all developers wishing to use ironSource's services must provide a company name at sign-up, and we observed companies with the following names sending them personal information: "Arial & Babies," "Androbaby," "Babies Funny World," "BabyBus Kids Games," "For Little Kids," "GameForKids," and "KidsUnityApps." From these developer names provided to ironSource, the resulting data was likely coming from children. However, ironSource can deny actual knowledge, so long as no human within the company looks at the data that they are soliciting from developers who use their services.

---

[44] Reyes *et al.*, *supra* note 3.

[45] Serge Egelman, "We get letters." The AppCensus Blog, May 10, 2018. https://web.archive.org/web/20240415123554/https:/blog.appcensus.io/2018/05/10/we-get-letters.

49. In addition, dark patterns—the strategic use of user interface designs to manipulate consumers into acting against their interests—are deployed across many commercial websites and other online services, and are often used to encourage consumers to spend additional money or time online, or to give up privacy.[46] Research shows that these techniques are prevalent in child-directed online services,[47] and that children are likely to be more susceptible to manipulations than adults.[48]

## III. CALIFORNIA'S PROTECTING OUR KIDS FROM SOCIAL MEDIA ADDICTION ACT

50. From my understanding of California's Protecting Our Kids from Social Media Addiction Act, I believe that the Act's requirements are technologically feasible and not onerous based on technology that is already in widespread use (including by NetChoice members).

51. The Act's requirement that content feeds not be based on information "associated with the user or the user's device"[49] is feasible to implement, because it involves simply modifying the algorithms that are already being used to curate content. These algorithms already exist and as noted earlier in this report, are often designed to consider personal information stored about the current user to make decisions. My understanding is that the Act would require that for minor users, these algorithms be replaced with ones that do not use information provided by the minor or from the minor's device. For example, instead of prioritizing the order of social media

---

[46] Fagan P. Clicks and tricks: The dark art of online persuasion. Curr Opin Psychol. 2024 Aug;58:101844. doi: 10.1016/j.copsyc.2024.101844. Epub 2024 Jul 10. PMID: 39029271.

[47] J. Radesky, A. Hiniker, C. McLaren, E. Akgun, A. Schaller, H. M. Weeks, S. Campbell, & A. N. Gearhardt (2022). "Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children." JAMA network open, 5(6), e2217641. https://doi.org/10.1001/jamanetworkopen.2022.17641.

[48] Dale Kunkel, Brian L. Wilcox, Joanne Cantor, Edward Palmer, Susan Linn, and Peter Dowrick. "Report of the APA task force on advertising and children." *Washington, DC: American Psychological Association* 30 (2004): 60.

[49] Cal. Health & Saf. Code §§ 27000.5, 27001.

posts shown to a user based on engagement metrics, a social media feed's algorithm could display posts chronologically. This should not be particularly onerous for social media providers to implement; indeed, some social media networks already offer users the choice over how to algorithmically curate their feeds. Bluesky, for example, allows users to choose from many different algorithms, as well as create their own,[50] and X, the social network formerly known as Twitter, offers users a choice between algorithmic recommendations from across the service or limiting content to followed accounts.[51]

52. The Act's requirement that push notifications not be shown to children during certain hours is similarly feasible and not onerous to implement.[52] Any device that supports push notifications also has a system clock and functionality for apps to check the local time without requiring any special permissions. That is, the user's local time is readily available to apps and other online services, and is already routinely collected by online services. When visiting websites, users' web browsers routinely transmit their users' time zones along with various other metadata. Similarly, on mobile devices, mobile apps routinely include the device's local time zone in their regular transmissions to their remote servers (as well as the servers of third parties). Thus, online services already have enough information at their disposal to determine a given user's local time zone; that logic can then be invoked in determining whether or not to display a push notification to a given user.

53. I believe that the Act's other requirements that pertain to certain controls and defaults are also technically feasible to implement. For example, many mobile devices and services already offer parental controls, including allowing parents to regulate hours of usage,[53]

---

[50] https://docs.bsky.app/docs/starter-templates/custom-feeds..

[51] https://help.x.com/en/using-x/x-timeline.

[52] Cal. Health & Saf. Code § 27002(a)(1).

[53] *Id.* § 27002(b)(1).

choose the feed algorithm,[54] the design of the user interface,[55] prohibit profiling of child users,[56] and configure basic privacy controls.[57] For example, Google—another NetChoice member—tells the developers of child-directed Android apps that they are prohibited from collecting location data or performing behavioral advertising.[58]

54. In many cases, the Act's requirements appear to overlap with requirements to which NetChoice's members are already subject to under COPPA. For example, COPPA requires that children's online services "must obtain verifiable parental consent before collecting any personal information from a child, unless the collection fits into one of the Rule's exceptions."[59] Thus, regulated entities under the Act may look to the FTC's guidance on how to obtain "verifiable parental consent" under COPPA.[60]

55. I understand that in certain cases, regulated entities under the Act will need to "reasonably determine" whether or not a user is a minor. This, too, is technically feasible and is a requirement in other jurisdictions in which NetChoice's members operate. For example, the European Parliament has put out guidance on how online services can perform age verification to comply with the Digital Services Act (DSA) and other EU regulations.[61] Online age verification need not be done in a manner that compromises users' privacy, either: CNIL, the French data

---

[54] *Id.* § 27002(b)(2).

[55] *Id.* § 27002b)(3).

[56] *Id.* § 27002(b)(4); COPPA already prohibits the use of a child's personal information for profiling (or targeted advertising) purposes.

[57] *Id.* § 27002(b)(5).

[58] https://support.google.com/googleplay/android-developer/answer/9893335?hl=en

[59] https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent.

[60] *Id.*

[61] https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.

protection agency, released a report two years ago documenting the different ways that age verification can be performed in a privacy-preserving manner.[62] Moreover, services need not worry about age verification if they simply adopt privacy-preserving default settings.

56. Overall, based on my knowledge and experience, I think that the Act's requirements are both technically feasible and not overly onerous; as I point out, many of NetChoice's members are already required to comply with substantially similar provisions in other jurisdictions.

## IV. TOOLS FOR LIMITING COLLECTION & USE OF PERSONAL INFORMATION

57. While some Internet web sites and social media companies impose voluntary online standards that purport to give consumers more control over their privacy, I have come to the conclusion that such voluntary measures are largely futile.

58. **Privacy Policies.** Internet users have few tools to control their online privacy. Since the dawn of the Internet age, the primary framework for managing online privacy has been the "notice and consent" framework, whereby online services post privacy policies ("notice") and consumers can choose whether to engage with services based on their understanding of those policies ("consent"). Unfortunately, this framework is fundamentally detached from reality: decades of research have demonstrated that consumers do not read these privacy policies, do not understand what they mean (when they do read them), and worse, privacy policies often do not accurately describe their services' behaviors.

59. In one study in which participants were asked to explicitly confirm that they read and agreed to a website's privacy policy, 80% clicked a box to affirm that they had done so despite not actually accessing or reading the policy.[63] This number likely represents a lower bound, given the presence of "demand characteristics" (i.e., participants were in a laboratory

---

[62] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

[63] Nili Steinfeld. "'I agree to the terms and conditions': (How) do users read privacy policies online? An eye-tracking experiment." *Computers in Human Behavior* 55 (2016): 992-1000.

setting and therefore were likely to pay more attention to the instructions than they likely would have in the real world), as well as the fact that most online services do not present users with interstitial messages demanding that they read and agree to their privacy policies: most privacy policies are accessed through discreet links outside the user's field of focus. Another study found that privacy-concerned users were influenced by the mere presence of a privacy policy link, despite few reading the policies.[64] This suggests that the mere presence of a privacy policy erroneously signals "good" privacy practices.

60. Nonetheless, if users do opt to read privacy policies, it is often a significant time investment. In 2008, McDonald and Cranor showed that if users read the privacy policies for every website they accessed, they would need to spend up to 300 hours per year doing so annually (based on average policy lengths, number of websites visited, and reading speeds).[65] Of course, their estimate is based on data from 2008 that showed the average Internet user visits around 1,500 unique websites annually; 15 years later, the number of websites has proliferated, as has the amount of time that consumers spend online, which suggests that the time investment to read and understand privacy policies has only increased.

61. It is also not clear that the time investment to read privacy policies is worthwhile for most consumers: several studies have shown that the privacy policies found on popular websites are written at the college level and therefore may not be understood by a significant proportion of the population (much less children).[66]

---

[64] Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: Self-reports versus observed behavior." *International Journal of Human-Computer Studies* 63, no. 1-2 (2005): 203-227.

[65] Aleecia M. McDonald and Lorrie Faith Cranor. "The cost of reading privacy policies." *I/S: A Journal of Law and Policy for the Information Society*, 4 (2008): 543.

[66] Yuanxiang Li *et al*. "Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment."

(continued…)

62. Even when policies are noticed, read, and understood, they generally do not explain a service's data practices in sufficient detail for consumers to make informed decisions. For example, despite CCPA and the California Online Privacy Protection Act requiring that services post privacy policies, there are no requirements that force those services to name the specific third parties with whom they share data—they are only required to specify the broad categories of data recipients. Even though those third parties may have their own data practices that are documented in their own privacy policies, it is nearly impossible for consumers to inform themselves about those practices if they are unable to locate those additional privacy policies because they do not know the identities of the companies. Similarly, it is nearly impossible for consumers to understand the privacy practices of large companies that offer multiple services, as their privacy policies are often written in a manner that aggregates their practices across all of their offered services (e.g., Google's privacy policy[67] describes their data collection practices across all of their services and does not convey what data may be collected by Google Maps vs. Gmail vs. Docs vs. Search).

63. **Blocking Cookies and Fingerprinting.** In addition to reading privacy policies, there are some technologies that consumers can use in futile attempts to better protect their privacy. "Cookies" are data that websites store in consumers' web browsers, which are then transmitted back to websites when visited in the future. This allows a website to recognize a user over time, without having to log in again (as well as allowing the website to "remember" other settings, such as a default language). Because cookies have been historically abused for invasive

---

*Communications of the IIMA* 12.3 (2012): 5; Carlos Jensen and Colin Potts. "Privacy policies as decision-making tools: an evaluation of online privacy notices." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 2004; George R. Milne, Mary J. Culnan, and Henry Greene. "A longitudinal assessment of online privacy notice readability." *Journal of Public Policy & Marketing* 25.2 (2006): 238-249.

[67] https://policies.google.com/privacy?hl=en-US.

tracking and profiling,[68] modern web browser software allows users to delete stored cookies or to block cookies set by third-party trackers altogether.

64. However, deleting or blocking cookies is no longer an effective strategy, as tracking now occurs using other means that consumers cannot control.[69] For example, unique "fingerprints"—the aggregation of several data points to create a unique identifier—can be constructed based on seemingly-benign information that is automatically transmitted to online services without user consent: software versions (e.g., the web browser and operating system), language settings, time zones, screen resolution, battery levels, etc.[70] Even what fonts are installed on a computer, which are available to websites, can be used to uniquely identify a website visitor.[71] Apps on mobile devices have additional data points available for constructing

---

[68] J. R. Mayer and J. C. Mitchell, "Third-Party Web Tracking: Policy and Technology," *2012 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, 2012, pp. 413-427, doi: 10.1109/SP.2012.47.

[69] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting," *2013 IEEE Symposium on Security and Privacy,* Berkeley, CA, USA, 2013, pp. 541-555, doi: 10.1109/SP.2013.43; R. Upathilake, Y. Li, and A. Matrawy, "A classification of web browser fingerprinting techniques," *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2015, pp. 1-5, doi: 10.1109/NTMS.2015.7266460.

[70] See, e.g., https://amiunique.org/; Peter Eckersley. "How unique is your web browser?" in *Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings 10*, pp. 1-18. Springer Berlin Heidelberg, 2010; Alex Hern. "Your battery status is being used to track you online." *The Guardian*, August 2, 2016, https://www.theguardian.com/technology/2016/aug/02/battery-status-indicators-tracking-online. Accessed: December 2, 2024.

[71] David Fifield and Serge Egelman. "Fingerprinting web users through font metrics."

(continued…)

unique fingerprints to identify their users, all without the use of cookies, and with few actions that users can take to prevent this from occurring. Perversely, whether a user has configured privacy settings away from the defaults is often used as a data point for further tracking (i.e., while some web browsers can transmit a user-configurable "do not track" signal to websites, many websites choose not to honor this and instead use it as another source of entropy to identify and track users).[72]

65. Every device connected to the Internet has an Internet Protocol (IP) address, which is used to route information to and from it. While IP addresses must be transmitted to send and receive data, they can also be used to track users over time. Since devices behind a firewall (e.g., a household WiFi router) will appear to the outside world to share the same IP address, the collection of IP addresses is often used as a way of performing "cross-device tracking," which allows data recipients to infer when the same individual has moved from using a mobile device to a desktop computer to a smart TV; it also allows data recipients to infer when multiple individuals reside within the same household. For example, Meta's privacy policy states that they collect "information about the network you connect your device to, including your IP address" to target advertisements and provide "business services" to unnamed partners.[73] There is little that consumers can do to prevent this, without substantially degrading their online experiences. Worse, there is no way for consumers to know when this type of tracking is even occurring.

---

*Financial Cryptography and Data Security: 19th International Conference, FC 2015*, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19. Springer Berlin Heidelberg, 2015.

[72] Geoffrey A. Fowler, "Think you're anonymous online? A third of popular websites are 'fingerprinting' you." *The Washington Post*, October 31, 2019. https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/; Michael Simon, "Apple is removing the Do Not Track toggle from Safari, but for a good reason." *Macworld*, February 6, 2019. https://www.macworld.com/article/232426/apple-safari-removing-do-not-track.html.

[73] https://www.facebook.com/privacy/policy/.

66. **Machine-Readable Privacy Policies.** Over 20 years ago, due to the privacy concerns regarding cookies, online tracking, and the acknowledgement that natural language privacy policies are woefully inadequate, several proposals were put forth to create machine-readable privacy policies. The idea behind these proposals was that consumers could use an interface to save their privacy preferences within their web browsers (or other software under their control), websites could post machine-readable policies, and then web browsers could act on consumers' behalf to either alert them when encountering a website with a disagreeable privacy policy (determined by the browser's automatic parsing of a website's machine-readable policy), or take some other action (e.g., automatically negotiating a better policy, blocking cookies or other transmissions, etc.). One of these proposals became a web standard: the Platform for Privacy Preferences Project (P3P),[74] was a web standard developed by the World Wide Web Consortium. (I served on the standards committee as an invited expert.)

67. The P3P standard gained traction, with many industry stakeholders adopting it by posting "P3P policies" on their websites so that web browsers could automatically parse them and alert users when they encountered websites that violated those users' stated privacy preferences. Microsoft's Internet Explorer (IE) browser was the first major web browser to adopt P3P, and by default, IE would block third-party tracking cookies unless the website posted a P3P policy (and then would block third-party cookies in accordance with the user's stated privacy preferences). In response, many companies (e.g., Amazon, Facebook, and Google) posted P3P policies that did not actually describe their privacy practices, but nonetheless tricked the IE browser into accepting their tracking cookies, due to the presence of a valid P3P header.[75] One study of over 33,000 websites observed that more than one third were transmitting P3P policies that appeared to be designed to circumvent IE's cookie blocking (and did not accurately describe their sites' actual

[74] https://en.wikipedia.org/wiki/P3P.

[75] Lorrie Faith Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice." *J. on Telecomm. & High Tech. L.* 10 (2012): 273.

privacy practices).[76] (The same study found that many of these websites were certified participants in TRUSTe's[77] EU Safe Harbor industry self-regulation program, and concluded that such certified sites were no more likely to comply with the P3P standard than websites not certified.) Some of these P3P policies can still be found today when accessing the websites that include trackers from NetChoice members.[78] For example, as of March 28, 2023, Google Ads[79] transmits a P3P policy header, but the body of the policy is as follows: CP="This is not a P3P policy! See g.co/p3phelp for more info."

**CONCLUSIONS**

68. For the reasons I set out in this declaration, I believe that the Act's provisions address a serious problem: the excessive use of social media by minors. It is also my professional opinion that the Act's requirements are technically feasible to implement. The technologies needed to comply with the Act's requirements already exist and, in many cases, are already in widespread use. Thus, complying with the Act will not create a new, onerous burden on regulated entities.

---

[76] Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M. McDonald, and Robert McGuire. 2010. Token attempt: the misrepresentation of website privacy policies through the misuse of p3p compact policy tokens. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society (WPES '10).* Association for Computing Machinery, New York, NY, USA, 93–104. https://doi.org/10.1145/1866919.1866932.

[77] TRUSTe is now known as "TrustArc."

[78] Lorrie Faith Cranor, "Internet Explorer privacy protections also being circumvented by Google, Facebook, and many more." *Technology Academics Policy,* February 18, 2021. https://www.techpolicy.com/Cranor_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx.

[79] https://adservice.google.com/adsid/google/ui.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 3, 2024, at Berkeley, California.

Serge Egelman, Ph.D.

# EXHIBIT A

# SergeEgelman

**contact**
2150 Shattuck Avenue
Suite 250
Berkeley, CA 94704
USA

egelman@cs.berkeley.edu

## education

| | | |
|---|---|---|
| 2009 | **PhD** in Computation, Organizations, and Society<br>School of Computer Science | Carnegie Mellon University |
| 2004 | **BS** in Computer Engineering<br>School of Engineering and Applied Science | University of Virginia |

## experience

| | | |
|---|---|---|
| | **AppCensus, Inc.** | San Francisco, CA |
| 2022–Now | Chief Scientist / Co-Founder | |
| 2019–2022 | CTO / Co-Founder | |
| | **International Computer Science Institute** | Berkeley, California |
| 2016–Now | Research Director, Usable Security & Privacy Group | |
| 2013–2016 | Senior Researcher, Networking and Security Group | |
| | **University of California, Berkeley** | Berkeley, California |
| 2011–Now | Research Scientist, Electrical Engineering and Computer Sciences | |
| | **National Institute of Standards and Technology** | Gaithersburg, Maryland |
| 2010–2011 | Research Scientist, Visualization and Usability Group | |
| | **Brown University** | Providence, Rhode Island |
| 2009-2010 | Postdoctoral Researcher, Computer Science Department | |
| | **Microsoft Research** | Redmond, Washington |
| 2008 | Research Intern, Security and Privacy Group | |
| 2008 | Research Intern, VIBE Group | |
| | **PARC** | Palo Alto, California |
| 2006 | Research Intern, Computer Science Laboratory | |

## publications*

### refereed journal publications

"Protect Me Tomorrow": Commitment Nudges to Remedy Compromised Passwords
*Peer, E., Frik, A., Gilsenan, C., and Egelman, S.* ACM Trans. Comput.-Hum. Interact. *(Aug. 2024). Association for Computing Machinery.*

The Medium is the Message:
How Secure Messaging Apps Leak Sensitive Data to Push Notification Services
*Samarin, N., Sanchez, A., Chung, T., Juleemun, A. D. B., Gilsenan, C., Merrill, N., Reardon, J., and Egelman, S.* Proceedings on Privacy Enhancing Technologies (PoPETS) *2024.4 (2024) pp. 967–982.*

*Over 13,000 citations and h-index=52: https://scholar.google.com/citations?hl=en&user=WN9t4n0AAAAJ

A Model of Contextual Factors Affecting Older Adults' Information-Sharing Decisions in the U.S.
*Frik, A., Bernd, J., and Egelman, S.* ACM Transactions on Computer-Human Interaction *30.1 (Apr. 2023). Association for Computing Machinery.*

Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA)
*Samarin, N., Kothari, S., Siyed, Z., Bjorkman, O., Yuan, R., Wijesekera, P., Alomar, N., Fischer, J., Hoofnagle, C., and Egelman, S.* Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2023).*

Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps
*Alomar, N., and Egelman, S.* Proceedings on Privacy Enhancing Technologies (PoPETS) *4 (2022) pp. 250–273.*

Data Collection Practices of Mobile Applications Played by Preschool-Aged Children
*Zhao, F., Egelman, S., Weeks, H. M., Kaciroti, N., Miller, A. L., and Radesky, J. S.* JAMA Pediatrics *174.12 (Dec. 2020).*

Nudge Me Right: Personalizing Online Security Nudges to People's Decision-Making Styles
*Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., and Frik, A.* Computers in Human Behavior *109 (Aug. 2020).*

Disaster Privacy/Privacy Disaster
*Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., and Egelman, S.* Journal of the Association for Information Science and Technology *(Mar. 2020).*

Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps
*Bamberger, K. A., Egelman, S., Han, C., Elazari, A., and Reyes, I.* Berkeley Technology Law Journal *35 (2020).*

The Price is (Not) Right: Comparing Privacy in Free and Paid Apps
*Han, C., Reyes, I., Feal, Á., Reardon, J., Wijesekera, P., Vallina-Rodriguez, N., Elazari, A., Bamberger, K. A., and Egelman, S.* Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2020).*

Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants
*Tabassum, M., Kosiński, T., Frik, A., Malkin, N., Wijesekera, P., Egelman, S., and Lipford, H. R.* Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technoligies (IMWUT) *3.4 (Dec. 2019). Association for Computing Machinery.*

Privacy Attitudes of Smart Speaker Users
*Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Wagner, D., and Egelman, S.* Proceedings on Privacy Enhancing Technologies *2019.4 (2019).*

"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale
*Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., and Egelman, S.* Proceedings on Privacy Enhancing Technologies *2018.3 (2018) pp. 63–83.* **Caspar Bowden PET Award**

A Usability Evaluation of Tor Launcher
*Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., and Wagner, D.* Proceedings on Privacy Enhancing Technologies *2017.3 (2017) pp. 87–106.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
*Tsai, J., Egelman, S., Cranor, L., and Acquisti, A.* Information Systems Research *22.2 (2011) pp. 254–268.* **AIS Best Publication of 2011 Award / INFORMS Best Published Paper Award (2012)**

P3P Deployment on Websites
*Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M., and Chowdhury, A.* Electronic Commerce Research and Applications *7.3 (2008) pp. 274–293.*

The Real ID Act: Fixing Identity Documents with Duct Tape
*Egelman, S., and Cranor, L. F.* I/S: A Journal of Law and Policy for the Information Society *2.1 (2006) pp. 149–183.*

**refereed conference publications**

Security and Privacy Failures in Popular 2FA Apps
*Gilsenan, C., Shakir, F., Alomar, N., and Egelman, S.* Proceedings of the 32nd USENIX Security Symposium *(USENIX Security '23), 2023.*

In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes
*Girish, A., Hu, T., Prakash, V., Dubois, D. J., Matic, S., Huang, D. Y., Egelman, S., Reardon, J., Tapiador, J., Choffnes, D., and Vallina-Rodriguez, N.* Proceedings of the 2023 ACM on Internet Measurement Conference *(IMC '23), 2023, New York, NY, USA.*

Log: It's Big, It's Heavy, It's Filled with Personal Data!
Measuring the Logging of Sensitive Information in the Android Ecosystem
*Lyons, A., Gamba, J., Shawaga, A., Reardon, J., Tapiador, J., Egelman, S., and Vallina-Rodriguez, N.* Proceedings of the 32nd USENIX Security Symposium *(USENIX Security '23), 2023.*

Can Humans Detect Malicious Always-Listening Assistants?
A Framework for Crowdsourcing Test Drives
*Malkin, N., Wagner, D., and Egelman, S.* Proceedings of the ACM Conference On Computer-Supported Cooperative Work And Social Computing *(CSCW '22), 2022, New York, NY, USA.*

Runtime Permissions for Privacy in Proactive Intelligent Assistants
*Malkin, N., Wagner, D., and Egelman, S.* Eighteenth Symposium on Usable Privacy and Security *(SOUPS 2022), 2022.*

"You've Got Your Nice List of Bugs, Now What?" Vulnerability Discovery and Management Processes in the Wild
*Alomar, N., Wijesekera, P., Qiu, E., and Egelman, S.* Proceedings of the Sixteenth Symposium on Usable Privacy and Security *(SOUPS 2020), 2020.*

Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with PoliCheck
*Andow, B., Mahmud, S. Y., Whitaker, J., Enck, W., Reaves, B., Singh, K., and Egelman, S.* 29th USENIX Security Symposium *(USENIX Security '20), 2020, Boston, MA.*

Don't Accept Candies from Strangers: An Analysis of Third-Party Mobile SDKs
*Feal, Á., Gamba, J., Tapiador, J., Wijesekera, P., Reardon, J., Egelman, S., and Vallina-Rodriguez, N.* International Conference on Computers, Privacy and Data Protection *(CPDP '20), 2020.*

A Qualitative Model of Older Adults' Contextual Decision-Making About Information Sharing
*Frik, A., Bernd, J., Alomar, N., and Egelman, S.* Workshop on the Economics of Information Security *(WEIS '20), 2020.*

Empirical Measurement of Systemic 2FA Usability
*Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., and Egelman, S.* Proceedings of the 29th USENIX Security Symposium *(USENIX Security '20), 2020.*

A Promise Is A Promise: The Effect of Commitment Devices on Computer Security Intentions
*Frik, A., Malkin, N., Harbach, M., Peer, E., and Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '19), 2019.*

Privacy and Security Threat Models and Mitigation Strategies of Older Adults
*Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., and Egelman, S.* Proceedings of the 15th Symposium on Usable Privacy and Security *(SOUPS '19), 2019, Berkeley, CA, USA.*

Information Design in An Aged Care Context
*Nurgalieva, L., Frik, A., Ceschel, F., Egelman, S., and Marchese, M.* Proceedings of the 13th International Conference on Pervasive Computing Technologies for Healthcare *(PervasiveHealth '19), 2019, New York, NY, USA.*

50 Ways to Leak Your Data:
An Exploration of Apps' Circumvention of the Android Permissions System
*Reardon, J., Feal, A., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S.* Proceedings of the 24th USENIX Security Symposium *(USENIX Security '19), 2019, Berkeley, CA, USA.* **USENIX**

**Security Distinguished Paper Award / AEPD Emilio Aced Personal Data Protection Research Award / CNIL-INRIA Privacy Award**

An Experience Sampling Study of User Reactions to Browser Warnings in the Field
*Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., and Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.*

Contextualizing Privacy Decisions for Better Prediction (and Protection)
*Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J.-W., Good, N., Wagner, D., Beznosov, K., and Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.* **SIGCHI Honorable Mention Award**

Let's go in for a closer look: Observing passwords in their natural habitat
*Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Forget, A.* Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '17), 2017, New York, NY, USA.*

Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences
*Tsai, L., Wijesekera, P., Reardon, J., Reyes, I., Egelman, S., Wagner, D., Good, N., and Chen, J.-W.* Proceedings of the 13th Symposium on Usable Privacy and Security *(SOUPS '17), 2017.*

The Feasibility of Dynamically Granted Permissions:
Aligning Mobile Privacy with User Preferences
*Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., and Beznosov, K.* Proceedings of the 2017 IEEE Symposium on Security and Privacy *(Oakland '17), 2017.*

Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes
*Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., and Telang, R.* Proc. of the 12th Symposium on Usable Privacy and Security *(SOUPS '16), 2016.*

Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)
*Egelman, S., Harbach, M., and Peer, E.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens
*Harbach, M., Luca, A. D., and Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking
*Harbach, M., Luca, A. D., Malkin, N., and Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Teaching Privacy Curriculum
*Egelman, S., Bernd, J., Friedland, G., and Garcia, D.* Proceedings of the 47th ACM technical symposium on Computer Science Education *(SIGCSE '16), 2016.*

Android Permissions Remystified: A Field Study on Contextual Integrity
*Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., and Beznosov, K.* 24th USENIX Security Symposium *(USENIX Security 15), 2015, Washington, D.C.*

Is This Thing On? Communicating Privacy on Ubiquitous Sensing Platforms
*Egelman, S., Kannavara, R., and Chow, R.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)
*Egelman, S., and Peer, E.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.* **SIGCHI Honorable Mention Award**

Fingerprinting Web Users through Font Metrics
*Fifield, D., and Egelman, S.* Proceedings of the 19th international conference on Financial Cryptography and Data Security *(FC'15), 2015.*

Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights
*Portnoff, R., Lee, L., Egelman, S., Mishra, P., Leung, D., and Wagner, D.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors
*Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., and Wagner, D.* Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '14), 2014, New York, NY, USA.*

The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior
*Tan, J., Nguyen, K., Theodorides, M., Negron-Arroyo, H., Thompson, C., Egelman, S., and Wagner, D.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '14), 2014, Toronto, Canada.*

The Importance of Being Earnest [in Security Warnings]
*Egelman, S., and Schechter, S.* Proceedings of the 17th international conference on Financial Cryptography and Data Security *(FC'13), 2013, Okinawa, Japan.*

My Profile Is My Password, Verify Me! The Privacy/Convenience Tradeoff of Facebook Connect
*Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection
*Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., and Herley, C.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources
*Thompson, C., Johnson, M., Egelman, S., Wagner, D., and King, J.* Proceedings of the Ninth Symposium on Usable Privacy and Security *(SOUPS '13), 2013, Newcastle, United Kingdom.*

Android permissions: user attention, comprehension, and behavior
*Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D.* Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.* **SOUPS Best Paper Award (2012) / SOUPS Impact Award (2017)**

Facebook and privacy: it's complicated
*Johnson, M., Egelman, S., and Bellovin, S. M.* Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.*

It's all about the Benjamins: Incentivizing users to ignore security advice
*Christin, N., Egelman, S., Vidas, T., and Grossklags, J.* Proceedings of the 15th international conference on Financial Cryptography and Data Security *(FC'11), 2011, Gros Islet, St. Lucia.*

Oops, I did it again: mitigating repeated access control errors on facebook
*Egelman, S., Oates, A., and Krishnamurthi, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.*

Of passwords and people: measuring the effect of password-composition policies
*Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.* **SIGCHI Honorable Mention Award**

Timing is everything?: the effects of timing and placement of online privacy indicators
*Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions
*Schechter, S., Brush, A. J. B., and Egelman, S.* Proceedings of the 2009 IEEE Symposium on Security and Privacy *(Oakland '09), 2009, Los Alamitos, CA, USA.*

It's not what you know, but who you know: a social approach to last-resort authentication
*Schechter, S., Egelman, S., and Reeder, R. W.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

Crying wolf: an empirical study of SSL warning effectiveness
*Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F.* Proceedings of the 18th USENIX Security Symposium *(SSYM'09), 2009, Montreal, Canada.*

Family accounts: a new paradigm for user accounts within the home environment

*Egelman, S., Brush, A. J. B., and Inkpen, K. M.* Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work *(CSCW '08), 2008, San Diego, CA, USA.*

You've Been Warned: An empirical study of the effectiveness of browser phishing warnings
*Egelman, S., Cranor, L. F., and Hong, J.* CHI '08: Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems *(CHI '08), 2008, Florence, Italy.* **SIGCHI Honorable Mention Award**

Phinding Phish: Evaluating Anti-Phishing Tools
*Zhang, Y., Egelman, S., Cranor, L. F., and Hong, J.* Proceedings of the 14th Annual Network & Distributed System Security Symposium *(NDSS '07), 2007, San Diego, CA.*

Power Strips, Prophylactics, and Privacy, Oh My!
*Gideon, J., Egelman, S., Cranor, L., and Acquisti, A.* Proceedings of the Second Symposium on Usable Privacy and Security *(SOUPS '06), 2006, Pittsburgh, PA.*

An analysis of P3P-enabled web sites among top-20 search results
*Egelman, S., Cranor, L. F., and Chowdhury, A.* Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet *(ICEC '06), 2006, Fredericton, New Brunswick, Canada.*

**refereed workshop publications**

Challenges in Inferring Privacy Properties of Smart Devices:
Towards Scalable Multi-Vantage Point Testing Methods
*Girish, A., Prakash, V., Egelman, S., Reardon, J., Tapiador, J., Huang, D. Y., Matic, S., and Vallina-Rodriguez, N.* Proceedings of the 3rd International CoNEXT Student Workshop *(CoNEXT-SW '22), 2022, Rome, Italy.*

Identifying and Classifying Third-Party Entities in Natural Language Privacy Policies
*Hosseini, M. B., Pragyan, K., Reyes, I., and Egelman, S.* Proceedings of the Second Workshop on Privacy in Natural Language Processing *(PrivateNLP '20), 2020.*

Do You Get What You Pay For? Comparing The Privacy Behaviors of Free vs. Paid Apps
*Han, C., Reyes, I., On, A. E. B., Reardon, J., Feal, A., Bamberger, K. A., Egelman, S., and Vallina-Rodriguez, N.* The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Privacy Controls for Always-Listening Devices
*Malkin, N., Egelman, S., and Wagner, D.* Proceedings of the New Security Paradigms Workshop *(NSPW '19), 2019, San Carlos, Costa Rica.*

On The Ridiculousness of Notice and Conset: Contradictions in App Privacy Policies
*Okoyomon, E., Samarin, N., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., Reyes, I., Feal, A., and Egelman, S.* The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Better Late(r) than Never: Increasing Cyber-Security Compliance by Reducing Present Bias
*Frik, A., Egelman, S., Harbach, M., Malkin, N., and Peer, E.* Workshop on the Economics of Information Security *(WEIS '18), 2018.*

"What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the U.S.
*Malkin, N., Bernd, J., Johnson, M., and Egelman, S.* Proceedings of the European Workshop on Usable Security *(EuroUSEC '18), 2018.*

Personalized Security Messaging: Nudges for Compliance with Browser Warnings
*Malkin, N., Mathur, A., Harbach, M., and Egelman, S.* Proceedings of the European Workshop on Usable Security *(EuroUSEC '17), 2017.*

"Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations
*Reyes, I., Wijesekera, P., Razaghpanah, A., Reardon, J., Vallina-Rodriguez, N., Egelman, S., and Kreibich, C.* The Workshop on Technology and Consumer Protection *(ConPro '17), 2017.*

Information Disclosure Concerns in The Age of Wearable Computing
*Lee, L. N., Lee, J. H., Egelman, S., and Wagner, D.* Proceedings of the NDSS Workshop on Usable Security *(USEC '16), 2016.*

The Myth of the Average User:
Improving Privacy and Security Systems through Individualization
*Egelman, S., and Peer, E.* Proceedings of the 2015 Workshop on New Security Paradigms *(NSPW '15), 2015, Twente, The Netherlands.*

Teaching Privacy: What Every Student Needs to Know
*Friedland, G., Egelman, S., and Garcia, D.* Proceedings of the 46th SIGCSE technical symposium on computer science education *(Workshop), 2015.*

U-PriSM 2: The Second Usable Privacy and Security for Mobile Devices Workshop
*Chiasson, S., Crawford, H., Egelman, S., and Irani, P.* Proc. of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services *(MobileHCI '13), 2013, Munich, Germany.*

Markets for Zero-day Exploits: Ethics and Implications
*Egelman, S., Herley, C., and Oorschot, P. C. van* Proceedings of the 2013 Workshop on New Security Paradigms Workshop *(NSPW '13), 2013, Banff, Alberta, Canada.*

Choice Architecture and Smartphone Privacy: There's A Price for That
*Egelman, S., Felt, A. P., and Wagner, D.* The 2012 Workshop on the Economics of Information Security *(WEIS '12), 2012, Berlin, Germany.*

How Good Is Good Enough? The sisyphean struggle for optimal privacy settings
*Egelman, S., and Johnson, M.* Proceedings of the Reconciling Privacy with Social Media Workshop *(CSCW '12 Workshop), 2012, Seattle, WA.*

It's Not Stealing if You Need It: A Panel on the Ethics of Performing Research Using Public Data of Illicit Origin
*Egelman, S., Bonneau, J., Chiasson, S., Dittrich, D., and Schechter, S.* Proceedings of the 16th International Conference on Financial Cryptography and Data Security *(FC'12), 2012.*

How to ask for permission
*Felt, A. P., Egelman, S., Finifter, M., Akhawe, D., and Wagner, D.* Proceedings of the 7th USENIX conference on Hot Topics in Security *(HotSec'12), 2012, Bellevue, WA.*

I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns
*Felt, A. P., Egelman, S., and Wagner, D.* Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices *(SPSM '12), 2012, Raleigh, North Carolina, USA.*

Toward Privacy Standards Based on Empirical Studies
*Egelman, S., and McCallister, E.* The Workshop on Web Tracking and User Privacy *(W3C Workshop), 2011, Princeton, NJ.*

Please Continue to Hold: An Empirical Study on User Tolerance of Security Delays
*Egelman, S., Molnar, D., Christin, N., Acquisti, A., Herley, C., and Krishnamurthi, S.* Workshop on the Economics of Information Security (WEIS '10) *(WEIS '10), 2010, Cambridge, MA.*

Tell Me Lies: A Methodology for Scientifically Rigorous Security User Studies
*Egelman, S., Tsai, J., and Cranor, L. F.* Proceedings of the Workshop on Studying Online Behavior *(CHI '10 Workshop), 2010, Atlanta, GA.*

This is Your Data on Drugs: Lessons Computer Security Can Learn from the Drug War
*Molnar, D., Egelman, S., and Christin, N.* Proceedings of the 2010 Workshop on New Security Paradigms *(NSPW '10), 2010, Concord, Massachusetts, USA.*

Security user studies: methodologies and best practices
*Egelman, S., King, J., Miller, R. C., Ragouzis, N., and Shehan, E.* CHI '07 Extended Abstracts on Human Factors in Computing Systems *(CHI EA '07), 2007, San Jose, CA, USA.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
*Tsai, J., Egelman, S., Cranor, L., and Acquisti, A.* Proceedings of the 2007 Workshop on the Economics of Information Security *(WEIS '07), 2007, Pittsburgh, PA, USA.*

Studying the Impact of Privacy Information on Online Purchase Decisions
*Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A.* Proceedings of the Workshop on Privacy and HCI: Methodologies for Studying Privacy Issues *(CHI '06 Workshop), 2006, Montreal, Canada.*

**book chapters and magazine articles**

50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System
Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. *;login:* 2019, USENIX Association.

Predicting Privacy and Security Attitudes
Egelman, S., and Peer, E. *Computers and Society*, 2015, ACM.

Crowdsourcing
Egelman, S., Chi, E., and Dow, S. *Ways of Knowing in HCI*, 2013, Springer.

Helping users create better passwords
Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Lopez, J. *;login:* 2012, USENIX Association.

Suing Spammers for Fun and Profit
Egelman, S. *;login:* 2004, USENIX Association.

Installation
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

User Administration
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

## awards and recognition

2022 **CNIL-INRIA Privacy Award**
*50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System*, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

**Emilio Aced Personal Data Protection Research Award**
*50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System*, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2020 **Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies**
*"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, with I. Reyes, P. Wijesekera, J. Reardon, A. Elazari, A. Razaghpanah, and N. Vallina-Rodriguez.

2019 **USENIX Security Symposium Distinguished Paper Award**
*50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System*, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2018 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
*Contextualizing Privacy Decisions for Better Prediction (and Protection)*, with P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, and K. Beznosov.

2017 **Symposium on Usable Privacy and Security (SOUPS) Impact Award**
*Android Permissions: User Attention, Comprehension, and Behavior*, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

**Elected ACM Senior Member** Association for Computing Machinery (ACM)

2016 **Symposium on Usable Privacy and Security (SOUPS) Distinguished Poster Award**
*Risk Compensation in Home-User Computer Security Behavior: A Mixed-Methods Exploratory Study*, with S. Pearman, A. Kumar, N. Munson, C. Sharma, L. Slyper, L. Bauer, and N. Christin.

**SIGCHI Honorable Mention Award (Best Paper Nominee)**
*Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)*, with M. Harbach and E. Peer.

**SIGCHI Honorable Mention Award (Best Paper Nominee)**
*The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens*, with M. Harbach and A. De Luca.

**SIGCHI Honorable Mention Award (Best Paper Nominee)**
*Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking*, with M. Harbach, A. De Luca, and N. Malkin.

2015 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
*Scaling the Security Wall: Developing a Security Behavior Intentions Scale*, with E. Peer.

2012 **AIS Best Publication of 2011**
*The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, with J. Tsai, L. Cranor, and A. Acquisti.

**ISR Best Published Paper**
*The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, with J. Tsai, L. Cranor, and A. Acquisti.

**SOUPS Best Paper Award**
*Android Permissions: User Attention, Comprehension, and Behavior*, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

2011 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
*Of Passwords and People: Measuring the Effect of Password-Composition Policies*, with S. Komanduri, R. Shay, P. G. Kelley, M. Mazurek, L. Bauer, N. Christin, and L. F. Cranor.

2008 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
*You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings*, with L. Cranor and J. Hong.

2006 **Tor Graphical User Interface Design Competition**
Phase 1 Overall Winner, with L. Cranor, J. Hong, P. Kumaraguru, C. Kuo, S. Romanosky, J. Tsai, and K. Vaniea.

**Publisher's Clearing House Finalist**
I *may* already be a winner.

## expert testimony and reports

2024 Expert witness for the plaintiffs in *Garner v. Amazon.com, Inc., No. 2:21-cv-00750 (W.D. Wash.)*. I provided a report and testimony explaining how in-home "virtual personal assistants" work, as well as explaining the associated privacy concerns based on the relevant research literature.

2024 Expert witness for the plaintiffs in *Lopez et al. v. Apple, Inc., No. 4:19-cv-04577-JSW (N.D. Cal.)*. I provided a report explaining how in-home "virtual personal assistants" work, as well as explaining the associated privacy concerns based on the relevant research literature.

2024 Expert witness for the plaintiffs in *Martinez et al. v. D2C, LLC d/b/a UNIVISION NOW, No. 1:23-cv-21394-RNS (S.D. Fla.)*. I provided a report and testimony explaining how the Meta Pixel functions and how it was used to transmit consumers' personally-identifiable information in violation of the Video Privacy Protection Act (VPPA).

2024 Expert witness for the plaintiffs in *Bloom v. Zuffa LLC, No. 2:22-cv-00412-RFB-BNW (D. Nev.)*. I provided a report and testimony explaining how the Meta Pixel functions and how it was used to transmit consumers' personally-identifiable information in violation of the Video Privacy Protection Act (VPPA).

2024 Expert witness for the plaintiffs in *Clark, et. al. v. Yodlee, Inc., No: 3:20-cv-05991-SK (N.D. Cal.)*. I provided a report and testimony explaining basic data protection concepts and consumer privacy expectations.

2024 Independent expert witness appointed by the court in *Czarnionka v. The Epoch Times Association, Inc., No. 1:22-cv-6348 (S.D.N.Y.)*. I was asked to perform a technical analysis to confirm that the terms of the injunctive relief were being followed.

2023-2024 Expert witness for the plaintiffs in *Frasco v. Flo Health, et al., No. 3:21-cv-00757 (N.D. Cal.)*. I provided an expert report and testimony based on my forensic analysis of a mobile app's data collection behaviors (i.e., privacy analysis). I was deposed and also provided rebuttal reports of opposing experts.

2023-2024 Expert witness for the California Department of Justice in *NetChoice, LLC v. Bonta, No. 5:22-cv-08861*. I provided a declaration opposing the motion to dismiss.

2022 Expert witness for the plaintiffs in *Hart, et al. v. TWC Product and Technology LLC, No. 4:20-cv-3842-JST*. I provided a rebuttal report and testimony about mobile app data collection behaviors.

2022 Expert witness for the District of Columbia Office of the Attorney General in *District of Columbia v. Town Sports International LLC*. I provided a rebuttal report and testimony on proper surveying methodology.

2021 Expert witness testifying before the U.S. Senate (Committee on Commerce, Science, and Transportation), hearing on "Protecting Kids Online: Internet Privacy and Manipulative Marketing." Testimony available at: https://www.commerce.senate.gov/2021/5/protecting-kids-online-internet-privacy-and-manipulative-marketing

2017-2019 Expert witness for the plaintiffs in *Vizio, Inc., Consumer Privacy Litigation, No. 8:16-ml-02693-JLS-KES*, assisting with discovery strategy and providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.

2016 Expert witness for the FTC in *FTC v. Amazon.com, Inc., No. C14-1028-JCC*, providing testimony on human-computer interaction (HCI) evaluation methods and critiquing opposing expert's report.

2014-2015 Expert witness for the plaintiffs in *Doe vs. Twitter, Inc., No. CGC-10-503630*, providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.

2014 Expert witness for the plaintiffs in *Levy v. Universal Parking of Florida, LLC No. 13-cv-22122 (S.D. Fla.)*, providing written testimony on basic human-computer interaction concepts as they relate to smartphone usage.

2013 Expert witness for the plaintiffs in *LinkedIn User Privacy Litigation, No. 12-cv-03088-EJD (N.D. Cal.)*, providing explanations of information security concepts and providing original research on users' privacy expectations in order to demonstrate and quantify damages.

2012 Expert witness for the plaintiffs in *Netflix Privacy Litigation, No. 5:11-cv-00379-EJD (N.D. Cal.)*, providing explanations of relevant privacy research and the economics of information privacy in order to quantify damages.

## grants awarded

2023–2026 **NSA: Improving Security and Safety of Neural Networks through Robust Training, Noise Augmentation, and Safety Metrics (H98230-23-C-0275)** $750,000
Co-PI (PI: Michael Mahoney, International Computer Science Institute)

2023–2026 **NSF: Measuring, Validating and Improving upon App-Based Privacy Nutrition Labels (CNS-2247951/2247952/2247953)** $600,000
Principal Investigator (Collaborative with Adam Aviv, George Washington University; Chris Kanich, University of Illinois at Chicago)

| | | |
|---|---|---|
| 2022–2025 | **NSF: Developer Implementation of Privacy in Software Systems (CCF-2217771/2217772)**<br>Principal Investigator (Collaborative with Primal Wijesekera, International Computer Science Institute; Jon Atwell and Julian Nyarko, Stanford University) | $750,000 |
| 2022–2026 | **KACST-UCB Center of Excellence for Secure Computing**<br>Senior Personnel (PI: David Wagner, University of California, Berkeley) | $6,460,000 |
| 2021–2022 | **CITRIS: Auditing the Compliance of California Consumer Privacy Regulations at Scale**<br>Principal Investigator (Collaborative with Zubair Shafiq, University of California, Davis) | $60,000 |
| 2019 | **Google: ASPIRE: SDK Traffic Identification at Scale**<br>Principal Investigator | $75,000 |
| 2018-2022 | **NSF: Mobile Dynamic Privacy and Security Analysis at Scale (CNS-1817248)**<br>Principal Investigator | $668,475 |
| 2018-2022 | **NSF: Contextual Integrity: From Theory to Practice (CNS-1801501/1801307/1801316)**<br>Principal Investigator (Collaborative with Helen Nissenbaum, Cornell University; and Norman Sadeh, Carnegie Mellon University) | $1,199,462 |
| 2018-2022 | **NSF: Increasing Users' Cyber-Security Compliance by Reducing Present Bias (CNS-1817249)**<br>Principal Investigator | $558,018 |
| 2018-2023 | **NSA: The Science of Privacy: Implications for Data Usage (H98230-18-D-0006)**<br>Principal Investigator (Co-PI: Michael Tschantz, International Computer Science Institute) | $3,236,424 |
| 2018-2019 | **DHS: Scaling Contextual Privacy to MDM Environments (FA8750-18-2-0096)**<br>Principal Investigator | $480,000 |
| 2018-2019 | **Rose Foundation: AppCensus: Mobile App Privacy Analysis at Scale**<br>Principal Investigator (Co-PI: Irwin Reyes, International Computer Science Institute) | $40,000 |
| 2018 | **Cisco: Access Controls for an IoT World**<br>Principal Investigator | $99,304 |
| 2018 | **CLTC: Privacy Analysis at Scale**<br>Principal Investigator | $50,000 |
| 2018 | **CLTC: Secure Internet of Things for Senior Users**<br>Co-PI (PI: Alisa Frik, International Computer Science Institute) | $60,590 |
| 2017 | **Mozilla: Towards Usable IoT Access Controls in the Home**<br>Principal Investigator | $46,000 |
| 2017 | **Data Transparency Lab (DTL) / AT&T: Transparency via Automated Dynamic Analysis at Scale**<br>Principal Investigator | $55,865 |
| 2017 | **CLTC: Secure & Usable Backup Authentication**<br>Co-PI (PI: David Wagner, University of California, Berkeley) | $48,400 |
| 2016 - 2017 | **NSF: Teaching Security in CSP (CNS-1636590)**<br>Co-PI (PI: Julia Bernd, ICSI) | $200,000 |
| 2016 - 2017 | **DHS: A Platform for Contextual Mobile Privacy (FA8750-16-C-0140)**<br>Principal Investigator | $664,378 |
| 2016 - 2018 | **CLTC: The Security Behavior Observatory**<br>Principal Investigator | $195,962 |
| 2016 | **CLTC: Using Individual Differences to Tailor Security Mitigations**<br>Principal Investigator | $100,000 |
| 2015 - 2018 | **NSF/BSF: Using Individual Differences to Personalize Security Mitigations (CNS-1528070/BSF-2014626)**<br>Principal Investigator (Collaborative with Eyal Peer, Bar-Ilan University) | $724,732 |

2015 - 2019 **NSF: Security and Privacy for Wearable and Continuous Sensing Platforms (CNS-1514211/1514457/1513584)** $1,200,000
Principal Investigator (Collaborative with David Wagner, University of California, Berkeley; and Franziska Roesner, University of Washington)

2014 - 2016 **NSF: Teachers' Resources for Online Privacy Education (DGE-1419319)** $300,000
Co-PI (PI: Gerald Friedland, ICSI)

2014 - 2017 **NSA: User Security Behavior** $200,000
Subcontract (PIs: Lorrie Cranor, Rahul Telang, Alessandro Acquisti, and Nicholas Christin; Carnegie Mellon University)

2014 **Google: Improving Security Warnings by Examining User Intent** $71,500
Principal Investigator

2013 - 2015 **NSF: Designing Individualized Privacy and Security Systems (CNS-1343433/1343451)** $132,620
Principal Investigator (Collaborative with Eyal Peer, Carnegie Mellon University)

2013 - 2016 **NSF: A Choice Architecture for Mobile Privacy and Security (CNS-1318680)** $500,000
Co-PI (PI: David Wagner, University of California, Berkeley)

2010 **Google: Designing Usable Certificate Dialogs in Chrome** $60,000
Principal Investigator

# patents awarded

2023 Automatic identification of applications that circumvent permissions and/or obfuscate data flows (US Patent 11,689,551)

# professional activities

### program committees

2024 IEEE Security & Privacy; Workshop on Economics and Information Security (WEIS); Contextual Integrity (CI) Symposium

2023 Privacy Enhancing Technologies Symposium (PETS); IEEE Security & Privacy; Workshop on Economics and Information Security (WEIS)

2022 Contextual Integrity (CI) Symposium

2021 Workshop on Economics and Information Security (WEIS)

2020 ACM CCS; Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS); USENIX Security

2019 Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS)

2018 ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS); IEEE Security & Privacy ("Oakland")

2017 ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Privacy Enhancing Technologies Symposium (PETS); New Security Paradigms Workshop (NSPW), **Co-Chair**; Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS)

| | |
|---|---|
| 2016 | Workshop on the Economics of Information Security (WEIS), **Chair**; New Security Paradigms Workshop (NSPW), **Co-Chair**; ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Symposium on Usable Privacy and Security (SOUPS); ACM WWW; Financial Cryptography and Data Security; Privacy Enhancing Technologies Symposium (PETS) |
| 2015 | Symposium on Usable Privacy and Security (SOUPS); USENIX Security; ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on the Economics of Information Security (WEIS); ACM WWW; Financial Cryptography and Data Security |
| 2014 | ACM SIGCHI (Human Factors in Computing Systems); Financial Cryptography and Data Security; ACM WWW; Privacy Enhancing Technologies Symposium (PETS) |
| 2013 | ACM SIGCHI (Human Factors in Computing Systems); Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Anti-Phishing Working Group eCrime Researchers Summit |
| 2012 | Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW) |
| 2011 | Symposium On Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Computers, Freedom, and Privacy (CFP) Conference (poster session co-chair); Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, **Co-Chair** |
| 2010 | Symposium On Usable Privacy and Security (SOUPS) |
| 2008 | Conference on Information and Knowledge Management (CIKM) |
| 2007 | ACM SIGCHI Workshop - Security User Studies: Methodologies and Best Practices; Anti-Phishing Working Group eCrime Researchers Summit (poster session co-chair) |
| 2006 | Computers, Freedom, and Privacy (CFP) Conference |

### standards committees

| | |
|---|---|
| 2007-2008 | W3C Web Security Context (WSC) Working Group |
| 2004-2006 | W3C Platform for Privacy Preferences (P3P) 1.1 Working Group |

### leadership roles

| | |
|---|---|
| 2024-Now | Advisory Board Member, Electronic Privacy Information Center (EPIC) |
| 2012-Now | Director, Berkeley Laboratory for Usable and Experimental Security (BLUES) |
| 2021-2023 | Member, ICSI Scientific Leadership Council |
| 2006-2008 | Legislative Concerns Chair / Board of Directors, National Association of Graduate and Professional Students (NAGPS) |
| 2006-2008 | Vice President for External Affairs, Carnegie Mellon Graduate Student Assembly |

## teaching

Fall 2019 **Usable Privacy and Security** University of California, Berkeley
Designed and taught a course as part of the School of Information's Masters in Cybersecurity program. Duties included course design and development, grading assignment and exams, supervising class projects, and holding office hours.

Spring 2017, Spring 2018 **Human Factors in Computer Security and Privacy** Brown University
Instructor for a module on "user interfaces for security" as part of the Executive Masters in Cybersecurity program. Duties included course design and development, grading assignments and exams, supervising thesis projects, and holding office hours.

Fall 2007 **Information Security & Privacy (46-861)** Carnegie Mellon University
Teaching assistant duties included developing course materials (topics for lectures, assignments, and exams), grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Spring 2006 **Computers and Society (15-290)** Carnegie Mellon University
Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Fall 2003 **Information Security (CS 451)** University of Virginia
Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, and holding office hours.

Fall 2003 **Intellectual Property (TCC 200)** University of Virginia
Teaching assistant duties included grading assignments and holding office hours.

Spring 2003, Spring 2004 **Advanced Software Development Methods (CS 340)** University of Virginia
Teaching assistant duties included grading and holding office hours.

Fall 2002 **Engineering Software (CS 201J)** University of Virginia
Teaching assistant duties included grading assignments and holding office hours.